Christopher I. Brain
cbrain@tousley.com
Kim D. Stephens
kstephens@tousley.com
Tousley Brain Stephens PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
Tel: 206.682.5600
Fax: 206.682.2992

Interim Lead Plaintiffs' Counsel

Keith S. Dubanevich
kdubanevich@stollberne.com
Steve D. Larson
slarson@stollberne.com
Stoll Stoll Berne Lokting & Shlachter P.C.
209 SW Oak Street
Portland, Oregon 97204
Tel: 503.227.1600
Fax: 503.227.6840

Interim Liaison Plaintiffs' Counsel

[Additional counsel appear on the signature page.]

UNITED STATES DISTRICT COURT

DISTRICT OF OREGON

PORTLAND DIVISION

IN RE PREMERA BLUE CROSS CUSTOMER DATA SECURITY BREACH LITIGATION This Document Relates to All Actions	Case No. 3:15-md-02633-SI **PLAINTIFFS' RESPONSE IN OPPOSITION TO PREMERA'S MOTION TO DISMISS**

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases **Page(s)**

Federal Statutes

State Statutes

Secondary Authorities

I. INTRODUCTION

This putative class action lawsuit arises from Defendant Premera Blue Cross's ("Premera") failure to safeguard the private and highly sensitive personal information of millions of members and users of Premera's heath care services – including their names, dates of birth, mailing addresses, telephone numbers, email addresses, Social Security numbers, member identification numbers, medical information, financial information, and other protected health information as defined by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") (collectively, "Sensitive Information"). The Sensitive Information Premera exposed to the hackers is not mere credit card numbers with no inherent privacy value. Rather, Premera disclosed medical data—some of the most personal and private information there is—to public view. This is the type of information people may not tell their closest friends, the type of information the law views as so confidential it is privileged from disclosure in litigation and legally protected by right of privacy torts. Class members reasonably expected, indeed some paid, Premera to safeguard this Sensitive Information, and Premera admittedly failed to do so.

Premera's lapse resulted in one of the largest healthcare data breaches in history, wherein Premera compromised the Sensitive Information of approximately 11 million people. Class members have been forced to take—and must continue to take—affirmative action to protect their Sensitive Information because of Premera's conduct. Seventeen of the 23 representative Plaintiffs named in the Consolidated Class Action Allegation Complaint (the "Complaint") have already experienced some form of data misuse—including instances of fraudulent financial activity (13), fraudulent tax returns (4), and/or phishing activity (5). The remaining six putative class representatives have spent their own time and money to minimize losses arising from further conversion of their Sensitive Information. The policyholder Plaintiffs did not receive what they paid for and reasonably expected—a health insurance plan accompanied by industry

standard (and legally required) data security protections.

Given Premera's demonstrated failure to safeguard its customers' and other consumers' Sensitive Information, Plaintiffs bring this action to recover:

(i) out of pocket or identity theft damages, such as loss of use of tax return funds and the time and money Plaintiffs spent minimizing their losses from further conversion of their Sensitive Information through credit monitoring and repair services;

(ii) value of their personal information, including the loss of their right to privacy by Premera's public disclosure of Plaintiffs' Sensitive Information; and

(iii) benefit of the bargain damages relating to the data protection services that the policyholder Plaintiffs paid for, reasonably expected, but did not receive.

In its Motion to Dismiss (the "Motion"), and consistent with its position at the October 29, 2015 hearing, Premera does not—for the most part—challenge Plaintiffs' ability to state a claim under any particular state's law (Def's Mot. at 11:7-21). Rather, the Motion asserts high-level challenges to certain elements of Plaintiffs' claims.

For the reasons discussed herein, Premera's Motion fails.

II. STATEMENT OF FACTS[1]

A. Premera's Business and Promises of Confidentiality and Data Security.

Premera is one of the largest healthcare insurance companies in the Pacific Northwest, and as part of the national Blue Cross Blue Shield Association, offers healthcare to more than 105 million Americans (Compl. ¶ 2). Premera is a Washington corporation with its principal

[1] Premera's short recounting of the facts it says are "material to the issues raised [in its Motion]" underscores its failure to respond to Plaintiffs' allegations. The Motion devotes only two cursory paragraphs to its statement of facts, but Premera still manages to squeeze in references to a supposed "subsequent investigation" wherein Premera claims that it determined that the intruders gained access to its systems, but that it has not yet "determined that any information was removed from [Premera's] system." (Mot. at 3, n. 1.) This material is extraneous to and found nowhere in Plaintiffs pleadings, and cannot be considered on a Rule 12(b)(6) Motion. *Lee v. City of Los Angeles*, 250 F.3d 668, 688 (9th Cir. 2001); *Rose v. JP Morgan Chase Bank, N.A.*, 835 F. Supp. 2d 1014, 1017 (D. Or. 2011) *aff'd sub nom.*, 542 F. App'x 585 (9th Cir. 2013) (same).

place of business in Mountlake Terrace, Washington (*Id.* ¶ 35). Its relevant operations, including its information security operations, are all located in Washington. (*Id*.)

In order to become a Premera member (or Blue Cross Blue Shield Association Network member ("Blue members") to receive healthcare services from a provider within the Premera network), an individual must give Premera his or her Sensitive Information, which Premera maintains in a centralized database in Washington. (*Id.* ¶¶ 3 and 35.) In recognition of the fact that reasonable consumers would expect Premera to protect the Sensitive Information, Premera promises and acknowledges its duty to safeguard and protect it. (*See, e.g., id.* ¶¶ 39-41.)

Premera emphasizes its promises and "commitment" to protect its customers' and Blue members' Sensitive Information in several public documents including its "Notice of Privacy Practices:"

> **THE PRIVACY OF YOUR MEDICAL AND FINANCIAL INFORMATION IS VERY IMPORTANT TO US.**
>
> At Premera Blue Cross, ***we are committed to maintaining the confidentiality of your medical and financial information***, which we refer to as your "personal information," regardless of format: oral, written, or electronic. . .
>
> **OUR RESPONSIBILITIES TO PROTECT YOUR PERSONAL INFORMATION**
>
> Under both the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Gramm-Leach-Bliley Act, ***Premera Blue Cross must take measures to protect the privacy of your personal information***. In addition, other state and federal privacy laws may provide additional privacy protection. Examples of your personal information include your name, Social Security number, address, telephone number, account number, employment, medical history, health records, claims information, etc.
>
> ***We protect your personal information in a variety of ways***. For example, we authorize access to your personal information by our employees and business associates only to the extent necessary to conduct our business of serving you, such as paying your claims. We take steps to secure our buildings and electronic systems from unauthorized access. We train our employees on our written confidentiality policy and procedures and employees are subject to discipline if they violate them. Our privacy policy and practices apply equally to personal information about current and former members; ***we will protect the privacy of your information even if you no longer maintain coverage through us***.

(Compl. ¶ 40, emphasis added). Premera further emphasized these commitments in its "Code of Conduct," which Premera makes publicly available through its website. (*Id.* ¶ 41.)

Without Premera's commitments to confidentiality and data security, Plaintiffs "would not have been willing to provide [Premera] with their Sensitive Information" at all, or otherwise pay Premera for "unsecured" healthcare insurance. (*Id.* ¶¶ 131-133.) Indeed, the risks of *not* securing patients' and consumers' Sensitive Information—*especially* of the sort at issue here—are well documented, given that "medical databases are particularly high-value targets for identity thieves." (*Id.* ¶¶ 68-77.) Premera's promises of data protection and its failure to disclose weaknesses in its cyber security were of material importance to all Plaintiffs. (*See, e.g., Id.* ¶¶ 39-42, 129, 162, 172) Likewise, those who paid for Premera insurance policies understood that Premera would use a portion of their premium payments to pay for those security measures. (*Id.* ¶ 67.)

B. Premera's Failure to Protect Plaintiffs' Sensitive Information Resulted in Its Loss and Misuse.

Premera failed to implement the data security that any reasonable consumer, including Plaintiffs, would expect, and for which Plaintiffs paid. This failure led to the massive exposure of Plaintiffs' Sensitive Information. (*Id.* ¶¶ 63-67.)

The attack on Premera's servers began in May 2014 with a low-tech phishing email. A Premera employee downloaded a fake "security update" that, once installed, provided hackers with an open door to Premera's servers. (*Id.* ¶ 46.) With this access, the hackers installed malware that remained in place until early 2015. (*Id.* ¶ 52.) Because Premera did not employ the necessary practices and tools at that time to protect its systems and to identify indicators of compromise and malware, Premera did not discover the breach until January 29, 2015. (*Id.*) Worse still, Premera did not notify the public about the breach—including affected consumers

and governmental authorities—until March 17, 2015. (*Id.* ¶ 57). Soon after, reports surfaced that "[t]hree weeks before hackers infiltrated Premera Blue Cross, federal auditors warned the company that its network-security procedures were inadequate," which "increase[d] the risk that vulnerabilities w[ould] not be remediated and sensitive data could be breached."[2]

C. Premera's Conduct Resulted in the Misuse of Plaintiffs' Sensitive Information and Caused an Imminent Risk of Harm.

As a result of Premera's conduct, seventeen of the named class representatives experienced some form of data misuse, while all were (and continue to be) exposed to a high risk of further, imminent injury. In response, all the named Plaintiffs suffered the loss of their Sensitive Information and spent money and time in an attempt to mitigate the harm caused (or in anticipation of future injuries). For the Court's convenience, the Plaintiffs' individual injuries are summarized in <u>Exhibit A</u>.

D. The Policyholder Plaintiffs Paid for Data Security They Never Received.

As paying members, policyholder Plaintiffs were required to provide Sensitive Information to Premera in exchange for Premera's promise to keep their personal and medical history private and secure in connection with their health insurance needs. (*Id*. ¶ 5.) Premera should have used some of Plaintiffs' payments to institute adequate protection of Plaintiffs' Sensitive Information, but Premera did not. (Compl. ¶ 67.) As a result, Premera exposed Plaintiffs' Sensitive Information during the data breach. (*Id*.) Policyholder Plaintiffs thus paid Premera for promised data security protections that they never received. (*See id.*) Had the policyholder Plaintiffs known of Premera's substandard methods of protecting their Sensitive

[2] (Mike Baker, *Feds Warned Premera About Security Flaws Before Breach*, Seattle Times, *available at* http://www.seattletimes.com/business/local-business/feds-warned-premera-aboutsecurity-flaws-before-breach/ (Oct. 6, 2015); *see also* Compl. ¶ 45.)

Information, they would have sought healthcare insurance coverage elsewhere. (*Id.* ¶ 9.)

III. ARGUMENT

A. All Plaintiffs Allege Cognizable Injuries.

Plaintiffs allege three categories of injuries and associated damages.[3] First, Plaintiffs allege out of pocket losses related to credit monitoring expenses, fraudulent accounts or tax returns, loss of use of money, and the time and effort Plaintiffs spent responding to Premera's failure to protect their Sensitive Information. Second, Plaintiffs allege damages inherent in the value of their personal information and the violation of their right to privacy – the damages that flow from disclosure of private Sensitive Information offensive to a reasonable person of ordinary sensibilities.[4] Third, the policyholder Plaintiffs allege benefit of the bargain damages related to money they paid to Premera for insurance coverage and data security. These damages are much greater than simple "over payment" damages as Premera mischaracterizes them. They stem from Premera's promise that it would protect its paying customers' Sensitive Information, and its failure to do so. As a result, the policyholder Plaintiffs lost the benefit of their bargain and suffered consequential damages by Premera's breach. Indeed, had Premera disclosed its true data security practices, the policyholder Plaintiffs would never have purchased health insurance from Premera in the first place.

Because Plaintiffs' claims for damages are sufficiently alleged and recoverable under any state's laws, Premera's Motion must be denied.

1. Plaintiffs allege compensable damages resulted from Premera's data

[3] Compare Premera's arguments in Motion at p. 18.
[4] *See, e.g.*, *Cowles Pub. Co. v. State Patrol*, 748 P.2d 597, 602 (Wash. 1988) ("Every individual has some phases of his life and his activities and some facts about himself that he does not expose to the public eye . . . for example . . . unpleasant or disgraceful or humiliating illnesses.") *See also*, Restatement (Second) of Torts § 652D.

breach.

a. *The nine Plaintiffs who allege misuse and economic damages also allege a plausible connection between the data breach and the resulting misuse of their Sensitive Information.*

Premera admits that those Plaintiffs who "experienced identity fraud that led to economic damages" allege cognizable injuries. (Mot. at 24.) Despite this, Premera still contends that these specific allegations of injury are not compensable because Plaintiffs only allege "a loose temporal connection between the alleged misuse [of their data] and the cyberattack[.]" (*Id.*) But Premera hardly addresses Plaintiffs' allegations, which draw several connections between the data breach and Plaintiffs' allegations of misuse. Premera is certainly entitled to try and disprove Plaintiffs' allegations of causation after discovery, but it cannot succeed in dismissing the Complaint by ignoring Plaintiffs' allegations.

The Seventh Circuit recently addressed the standard for alleging a causal connection between a data breach and allegations of harm. In *Remijas v. Neiman Marcus Grp., LLC,* 794 F.3d 688, 690-91 (7th Cir. 2015) the plaintiffs alleged (i) a temporal element (i.e., that they "incurred fraudulent charges on [their credit or debit accounts] after [they] used [them] at Neiman Marcus"), (ii) that Neiman Marcus notified them that their data had been compromised, and (iii) that Neiman Marcus offered them "one year of free credit monitoring and identity-theft protection." *Remijas*, 794 F.3d at 690-91. In addressing whether the plaintiffs had alleged a plausible connection between the data breach and their alleged damages, the court explained:

> The fact that Target or some other store *might* have caused the plaintiffs' private information to be exposed does nothing to negate the plaintiffs' standing to sue … **It is enough at this stage of the litigation that Neiman Marcus admitted that 350,000 cards might have been exposed and that it contacted members of the class to tell them they were at risk.** Those admissions and actions by the store adequately raise the plaintiffs' right to relief above the speculative level.

Id. at 696 (emphasis added, internal citations omitted). Indeed, the court went on to note that

where multiple companies may have exposed plaintiffs' private information to hackers, "the common law of torts has long shifted the burden of proof to defendants to prove that their negligent actions were not the 'but-for' cause of the plaintiff's injury." *Id*.

The Ninth Circuit has followed a similar view of standing. In *Stollenwerk*, the plaintiff claimed that his personal information was compromised as a result of the theft of a computer hard drive, which he claimed the defendant had negligently failed to secure, resulting in identity theft including the opening of fraudulent credit accounts. *Stollenwerk v. Tri-W. Health Care All.*, 254 F. App'x 664, 665 (9th Cir. 2007). The court observed that "while *purely* temporal connections are often insufficient to establish causation . . . proximate cause [can be] supported not only by the temporal, but also by the *logical*, relationship between . . . two events." *Id.* at 668 (emphasis in original). The court explained:

> 'Circumstantial evidence, expert testimony, or common knowledge may provide a basis from which the causal sequence may be inferred.... Such questions are peculiarly for the jury; ... [and] are questions on which a court can seldom rule as a matter of law.' As a matter of twenty-first century common knowledge, just as certain exposures can lead to certain diseases, the theft of a computer hard drive certainly *can* result in an attempt by a thief to access the contents for purposes of identity fraud, and such an attempt *can* succeed.

Id. (quoting *Wisener,* 598 P.2d at 513) (emphasis in original). *Accord* William Prosser, Law of Torts, § 41, 242-243 (4th Ed. 1971). The Ninth Circuit also explained that "the fact that the *type of information* [compromised] is the same kind needed to open credit accounts at the stores where these incidents took place is a matter of common knowledge from which a jury could reasonably draw inferences regarding its probative value in establishing causation." *Id.* at 667 (emphasis in original) (citing *Wisener,* 598 P.2d at 513).

Plaintiffs demonstrate a sufficient causal connection between the Premera data breach and their allegations of misuse of that data under *Remijas* and *Stollenwerk.* As in *Remijas*, each alleges (i) a temporal element (i.e., that each provided Sensitive Information to Premera before

the data breach, and experienced identity theft after the data breach) and (ii) that each received notification from Premera that his or her Sensitive Information had been compromised along with an offer of the credit monitory services. (Compl. ¶¶ 3, 6, 57-58.) Further, consistent with *Stollenwerk*, it's a "matter of common knowledge" that the Sensitive Information (which includes financial information, Social Security numbers, and other data) unlawfully accessed during Premera's breach is the same type of information needed to perpetrate the identity theft that the Plaintiffs experienced. Plaintiffs' allegations are more than sufficient to survive a motion to dismiss. *See In re Target Corp. Data Sec. Breach Litig.*, 66 F. Supp. 3d 1154, 1159 (D. Minn. 2014) (finding plaintiff's allegations sufficient for purposes of FRCP 12(b)(6) and stating, "[s]hould discovery fail to bear out Plaintiffs' allegations, Target may move for summary judgment on the issue.").

b. *All class members allege recoverable loss of "time and money" and the lost value of personal information resulting from Premera's faulty data security practices.*

It is well-established that a data breach victim alleges a cognizable injury where he or she suffers actual identity theft or data misuse, including where "accounts [are] opened in [the plaintiff's] name," *Resnick v. AvMed, Inc.*, 693 F.3d 1317, 1322 11th Cir. 2012); *In re Target Corp. Data Sec. Breach Litig.*, 66 F.Supp. 3d at 1159. (reasoning that cognizable injuries include "unlawful charges"); and *Ponder v. Pfizer, Inc.*, 522 F. Supp. 2d 793, 798 n.5 (M.D. La. 2007) (cognizable injury occurs where "the compromised data are used by a third party to steal someone's identity."). Moreover, once a data breach victim has suffered data misuse, she may also recover damages for costs expended to "sort[] things out" and address additional, future potential harms. *Remijas*, 794 F.3d at 692; *see also Anderson v. Hannaford Bros. Co.*, 659 F.3d 151, 165-67 (1st Cir. 2011) (finding it reasonable and foreseeable that a victim of identity theft would take steps to mitigate the consequences); *Witriol v. LexisNexis Grp.*, No. 05-cv-02392

MJJ, 2006 WL 4725713, at *6 (N.D. Cal. Feb. 10, 2006) (holding costs associated with monitoring and repairing credit compensable); *Kuhn v. Capital One Fin. Corp.*, No. 05-P-810, 2006 WL 3007931, at *3 (Mass. App. Ct. 2006) (holding time spent attempting to undo actual identity theft compensable).[5]

Premera argues that only plaintiffs who suffer misuse *and* allege out-of-pocket losses have claims (Mot. at 21-24). Premera's argument fails because it is based on the faulty premise that Plaintiffs have no protectable right of privacy in an inherent loss from exposure of their Sensitive Information. *See infra* at Section III A. Moreover, Premera allowed hackers to steal some of the most valuable purloined information because the Sensitive Information contained Social Security numbers, dates of birth, employer and income information. The Ninth Circuit has recognized California law permits damages for harm caused by the "dissemination of personal information" and "losing the sales value of that information" in far less egregious circumstances. *In re Facebook Privacy Litig.*, 572 Fed. App'x 494 (9th Cir. 2014).

Furthermore, Premera ignores that a cognizable injury may arise where (i) a data breach causes significant risk of future harm, and (ii) the mitigation efforts taken in response to that risk are reasonable. *See Anderson*, 659 F.3d at 164. From this standpoint, whether there was actual misuse of information is irrelevant; the question is whether the risk caused by the data breach "entitle[s] [Plaintiffs] to recover for expenditures reasonably made or harm suffered in a reasonable effort to avert the harm threatened." *See* Rest. (2d) of Torts § 919(1). *See also*

---

[5] Courts have also found that, as some Plaintiffs allege here, (*See* Compl. ¶¶ 96, 136, 157, 203, 211, 226, 235), a data breach victim suffers damages where identity theft leads to a diminished credit score. *See, e.g.*, *Kim v. Riscuity, Inc.*, No. 06-cv-1585, 2006 WL 2192121, at *2 (N.D. Ill. July 31, 2006) (finding damage to credit score actual injury); *Allen v. CitiMortgage, Inc.*, No. 10-cv-2740, 2011 WL 3425665, at *10 (D. Md. Aug. 4, 2011) (same); *Stagikas v. Saxon Mortg. Services., Inc.*, 795 F. Supp. 2d 129, 137 (D. Mass. 2011) (same).

Anderson, 659 F.3d at 162 ("To recover mitigation damages, plaintiffs need only show that the efforts to mitigate were reasonable, and that those efforts constitute a legal injury, such as actual money lost[.]" (internal citation omitted)); *Corona v. Sony Pictures Ent., Inc.*, No. 14-cv-09600, 2015 WL 3916744, at *4 (C.D. Cal. June 15, 2015) (finding that plaintiffs "sufficiently allege[d] facts to support the reasonableness and necessity of Plaintiffs' credit monitoring"); *Kuhn*, 2006 WL 3007931, at *3 (data breach victim was "entitled to recover for expenditures reasonably made or harm suffered in a reasonable effort to avert the harm threatened," including "the value of the time spent in seeking to prevent or undo the harm." (Quoting Rest. (2d) of Torts § 919)); *Jones v. Commerce Bancorp, Inc.*, No. 06-cv-835, 2006 WL 1409492, at *2 (S.D.N.Y. May 23, 2006) (finding that allegations of a cancelled insurance policy, lost income, and time spent remedying fraudulent withdrawals satisfied the damages element of negligence). Further, as to Plaintiffs' Washington Consumer Protection Act claims, the Washington State Supreme Court has expressly held that costs incurred investigating the harm resulting from a CPA violation is a cognizable injury, even without other harm. *Panag v. Farmers, Ins. Co. of Washington*, 204 P.3d 885, 902-03 (Wash. 2009); *see also*, *State Farm Fire and Cas. Co. v. Huynh*, 962 P.2d 854, 862 (Wash. Ct. App. 1998) (expenses incurred investigating false billing reports constituted injury even though the insurance company did not incur the loss of paying the false bills). [6]

Here, the exposure of Plaintiffs' Sensitive Information has put them at high risk for identity theft; indeed, most named Plaintiffs have experienced data misuse already. (Compl. ¶ 8.) Further, all Plaintiffs received letters in March 2015 notifying them that their Sensitive Information may have been compromised, and offering to provide free credit and identity

[6] Plaintiffs and the putative class may all bring a claim under the Washington CPA, even as out-of-state residents. *Thornell v. Seattle Serv. Bureau, Inc.*, --- P.3d ---, 2015 WL 8546860, at * (Wash. 2015).

protection services. (*Id.* ¶¶ 78-80, 82-89, 91, 94, 95, 100.) Even without *actual* misuse of data, these same facts provide "a reasonable basis for fearing" that a plaintiff would suffer identity theft or other misuse as a result of the data breach, so as to justify mitigation efforts. *See Anderson*, 659 F.3d at 166. *See also Corona*, 2015 WL 3916744, at *4 (facts justifying mitigation efforts included: (i) type of data exposed (SSNs, financial information, health insurance/medical information), (ii) the increased risk of identity theft to plaintiffs "relative to the time period before the breach, as well as to the risk born by the general public," (iii) that "consequences resulting from identity theft can be both serious and long-lasting," and (iv) that "some plaintiffs have already received notification of attempted identity theft." (citing *Potter v. Firestone Tire & Rubber Co.*, 863 P.2d 795 (Cal. 1993).); *Remijas*, 794 F.3d at 694 ("It is telling … that Neiman Marcus offered one year of credit monitoring and identity-theft protection to all customers. It is unlikely that it did so because the risk is so ephemeral that it can safely be disregarded.").

Fundamental policy concerns also "encourage[] plaintiffs to take reasonable steps to minimize losses" caused by a defendant. *Anderson*, 659 F. 3d at 162. The Plaintiffs who have spent money on credit monitoring or have expended time addressing fraudulent credit and tax activity should not be penalized for taking necessary and reasonable steps to protect against identity theft and further losses – such steps having only been taken as a result of Premera's conduct in failing to safeguard Plaintiffs' Sensitive Information.[7] (Compl. ¶¶ 136, 157, 203, 211,

[7] These allegations distinguish this case from those that Premera cites for the proposition that Plaintiffs' reliance on a speculative future injury does not support a claim for damages. *See, e.g.*, *Pisciotta*, 499 F.3d at 632; *Krottner*, 406 F. App'x at 131. In both *Pisciotta* and *Krottner* the courts found no cognizable injury because the plaintiffs failed to allege a loss related to their mitigation attempts. Here Plaintiffs *do* allege loss—both in money and time expended trying to remedy or mitigate damage caused by the Premera data breach in addition to alleging loss of the benefit of their bargain. *Cf. Anderson* 659 F.3d at 166 (distinguishing *Pisciotta* on this basis).

226, 235.) This is especially true here given the extreme and lasting harm that often results from compromised *medical* data. (*Id*. ¶ 7.) *See also Corona*, 2015 WL 3916744, at *5.

2. The Policyholder Plaintiffs' benefit of the bargain damages are sufficiently alleged and recoverable.

The Policyholder Plaintiffs' claims for damages are straightforward. They allege that they (i) paid Premera for services (including both health insurance and data security), (ii) did not receive everything for which they paid (data security), and, (iii) were damaged as a result. Premera contorts the pleadings claiming the Policyholder Plaintiffs cannot recover because their "overpayment" damages aren't causally linked to the data breach and are barred by the "filed rate doctrine." Both challenges fail.

a. *Premera's "causation" challenge does not address the pleadings.*

Premera's argument—that benefit of the bargain damages are not recoverable because they did not "result from" the data breach—misses the point of the Policyholder Plaintiffs' claims. First, all of the Policyholder Plaintiffs *do* allege more "traditional" data breach damages (e.g., out-of-pocket expenses relating to fraudulent accounts and efforts to mitigate further injury). Policyholder Plaintiffs *also* allege that because they paid for services they did not receive (and never would have purchased from Premera had they known of its actual data security practices), they were harmed in that way as well. (Compl. ¶¶ 8-9.) Premera cannot contest this theory of recovery by refusing to address it. Indeed, data breach cases have applied a "would not have purchased" theory of recovery—i.e., had a defendant been forthright about its actual data security practices, plaintiffs never would have purchased a given service or product in the first place. *See, e.g., In re Target*, 2014 WL 7192478, at *22-23 (accepting damages theory alleging that plaintiffs "would not have shopped" had they known about the Target's data security issues).

Courts have also recognized the benefit of the bargain measure of damages where

plaintiffs paid for promises of data security - typically communicated through a privacy policy or other documents – but did not receive the promised security. *See, e.g.*, *Resnick*, 693 F.3d at 1328 (data breach case endorsing benefit of the bargain damages on unjust enrichment claim, on allegations that health insurer failed to use money for data security in accordance with privacy notices); *Weinberg v. Advanced Data Processing, Inc.*, No. 15-CIV-61598, 2015 WL 8098555, at *6 (S.D. Fla. Nov. 17, 2015) (data breach case against medical payment processor following *Resnick*); *Doe 1 v. AOL LLC*, 719 F. Supp. 2d 1102, 1105 (N.D. Cal. 2010) (allowing benefit of the bargain damages in case involving public disclosure of sensitive information from AOL); *In re Adobe Sys., Inc. Privacy Litig.*, 66 F. Supp. 3d 1197, 1224 (N.D. Cal. 2014) (denying motion to dismiss where plaintiffs alleged they paid more for Adobe products than they would have had they known Adobe was not providing the reasonable security it represented).

Here, the Policyholder Plaintiffs assert both theories. First, Plaintiffs allege that because Premera did not provide Plaintiffs with all that they paid for (i.e., insurance coverage *and* data security), they were harmed. (Compl. ¶¶ 160-184). This theory supports Plaintiffs' claims sounding in contract or quasi-contract, *see, e.g.*, *Resnick*, 693 F.3d at 1328, as well as claims brought under the Washington CPA, *see Erickson v. Upjohn Co.*, 78 F.3d 592 (9th Cir. 1996) (recognizing even if plaintiff "had not suffered any physical injury from the [purchased] drug, she still would have had a [CPA] claim against [defendant] if, as is alleged here, she spent money on [the drug] and it did not work as advertised."); *see also Mason v. Mortg. American, Inc.*, 792 P.2d 142, 148 (Wash. 1990) ("The injury element [of a Washington CPA claim] will be met if the consumer's property interest or money is diminished because of the unlawful conduct even if the expenses caused by the statutory violation are minimal.").

Second, Plaintiffs allege that but for Premera's misrepresentations and omissions, the policyholder Plaintiffs never would have purchased Premera's services in the first place. This theory supports the Plaintiffs' claims for unjust enrichment and satisfies the causation requirement of the Washington CPA. *See Indoor Billboard/Washington, Inc. v. Integra Telecom of Washington, Inc.*, 170 P.3d 10, 21-22 (Wash. 2007) (finding that CPA's causation element was satisfied because "but for the defendant's inflated appraisal, the plaintiffs would not have made the [at-issue] investment." (internal quotation omitted)).

b. *The filed rate doctrine does not insulate Premera from liability for its failure to implement required cyber security.*

Premera is mistaken in asserting that the filed rate doctrine has any applicability in this case. Under the "court created 'filed rate doctrine,' once an agency approves a rate, such as a health insurance premium, courts will not reevaluate that rate because doing so would inappropriately usurp the agency's role." *McCarthy Finance, Inc. v. Premera*, 347 P.3d 872, 873 (Wash. 2015).

The filed rate doctrine applies only to "'allegations concerning the reasonableness of the filed rates.'" *McCarthy*, 347 P.3d at 875 (quoting *Tenore*, 136 Wash. 2d at 331-32). As the *McCarthy* court recognized, "courts may consider claims that are related to rates approved by an agency but do not require the courts to reevaluate such rates." *Id.* at 873; *see also Adamson v. WorldCom Comm. Inc.*, 78 P.3d 577, 582 (Or App 2003) ("The filed-rate doctrine bars only an action that seeks to vary the terms of an applicable tariff. . . . [M]erely because a tariff exists does not necessarily mean that a claim is barred."); *Facaros v. Qwest Corp.*, No. 10-cv-6343, 2011 WL 2270588, at *3 (D. Or. 2011) (holding filed rate doctrine did not apply where tariff regulating "construction" charges did not apply to defendant's bills for moving telephone wires). Consistent with this view, the *Adamson* court rejected defendant phone companies' reliance on

the filed rate doctrine in a case where the plaintiff wasn't disputing the "reasonableness" of a given rate, but rather, alleged the defendants had wrongfully charged him for a service for which he paid and did not receive. *Adamson*, 78 P.3d at 580, 582.

Unlike *McCarthy*, the Policyholder Plaintiffs here do not allege that Premera made any "excessive overcharges for premiums." *McCarthy*, 347 P.3d at 874.[8] Rather, Plaintiffs allege that Premera wrongfully charged them for a service (cyber security) that was not provided. The filed rate doctrine does not apply in this case, as it might if Plaintiffs were challenging the *amount* of the premiums charged. *See Id.* at 875 ("The mere fact that a claim is related to an agency-approved rate is no bar."); *Perryman v. Litton Loan Servicing, LP*, No. 2014 WL 49546, at *9 (N.D. Cal. Oct. 1, 2014) ("Plaintiff does not dispute the reasonableness of rates charged for insurance . . . [but] the amount of that rate which can be passed on to her under the terms of her contract with Defendants."). Plaintiffs were willing to (and did) pay the full amount of the premiums, but justifiably expected that Premera would use a portion of such payments to implement required security. (Compl. ¶¶ 62-67.) Premera breached its contract with Plaintiffs and is liable for the loss of the benefit of their bargain as well as consequential damages.

B. Premera's Remaining Challenges to Plaintiffs' Claims Are Ineffective.

1. Premera's challenge to Plaintiffs' misrepresentation and omission claims fails.

Premera attacks Plaintiffs' misrepresentation and omission claims by arguing that they

[8] The only case other than *McCarthy* that Premera cites in support of its invocation of the filed rate doctrine is equally inapplicable. In *Weinberg v. Sprint Corp.*, 801 A.2d 281 (N.J. 2002) (cited in Mot. at 18), plaintiffs challenged a long-distance phone carrier's practice of "rounding up" the federally filed "per-minute charge" for its services. *Id.* at 284. But Plaintiffs here do not "seek to enforce a rate other than the filed rate." *See id.* at 286. Rather, Plaintiffs seek to recover that portion of their premium payments that Premera should have spent, but failed to spend, on the required, reasonable cyber security measures that could have prevented the data breach and protected class members' confidential information.

are not "pled with particularity." As an initial matter, Rule 9(b) does not apply to Plaintiffs' claims. However, even if it did, Plaintiffs have alleged their claims with sufficient particularity to survive any pleading standard.

a. *Rule 9(b)'s heightened pleading requirements do not govern Plaintiffs' misrepresentation and omission claims.*

First, the entire premise of Premera's argument against Counts 1, 7, and 11—that because all of Plaintiffs' CPA and omission based claims "allege fraud, Rule 9(b) requires that they be pled with particularity," (Mot. at 4)—is in error.

Plaintiffs' Washington CPA claim focuses on Premera's unfair acts and omissions and does not require proof of intent or knowledge that the at-issue misrepresentations were false or misleading; instead, it requires only an unfair or deceptive act or practice. The CPA claim "does not sound in fraud." *Kreidler v. Pixler*, No. 06-cv-0697, 2006 WL 3539005, at *11 (W.D. Wash. Dec. 7, 2006). *See also Vernon v. Qwest Comm. Int'l, Inc.*, 643 F. Supp. 2d 1256, 1265 (W.D. Wash. 2009) ("Fraud is not an essential element of Plaintiffs' unjust enrichment or consumer protection act claims under Washington or Minnesota law because Plaintiffs have not alleged facts that constitute fraud and the gravamen of the complaint is not fraud.").[9]

Relatedly, Plaintiffs' claims that stem from Premera's alleged omissions "can succeed without the same level of specificity required by a normal fraud claim." *See MacDonald v. Ford Motor Co.*, 37 F. Supp. 3d 1087, 1096 (N.D. Cal. 2014) (internal citations omitted) ("a plaintiff alleging an omission-based fraud will 'not be able to specify the time, place, and specific content

[9] The same is true of certain other states' consumer protection statutes, particularly where a claim stems from a defendant's unfair or unlawful (rather than fraudulent) conduct. *See, e.g., Pelman ex rel. Pelman v. McDonald's Corp.*, 396 F.3d 508, 511 (2d Cir. 2005) (discussing New York General Business Law § 349); *Tatum v. Oberg*, 650 F. Supp. 2d 185, 195 (D. Conn. 2009) (discussing Connecticut Unfair Trade Practices Act).

of an omission as would a plaintiff in a false representation claim.'").[10] For such claims, "the plaintiff may find alternative ways to plead the particular circumstances of the fraud." *Barber*, 2014 WL 3529766, at *11 (internal citations and quotations omitted)). For example, "[a] plaintiff [can plead] justifiable reliance just by alleging that a reasonable customer would not have paid the asking price had the defect been disclosed." *Gray*, 22 F. Supp. 3d at 385 (citing *Falk*, 496 F. Supp. 2d at 1099).

Thus, Premera's reliance on Rule 9(b) is misplaced. In any event, and as explained below, Plaintiffs' claims under the states' consumer protection statutes and for misrepresentation by omission are pleaded with particularity, readily satisfying any standard.

b. *Plaintiffs identify actionable misrepresentations (and do so with particularity to the extent required).*

Premera contends that Plaintiffs have not "plausibly alleged" any misrepresentations regarding data security. (Mot. at 5.) While Premera admits its documents are replete with references to Premera's "commitment" to safeguard its customers' data, Premera says that its written statements fall short of a "guarantee that private information on Premera's data network would never be wrongfully accessed." (*Id.*) Plaintiffs have not asserted that Premera made any "guarantee". Rather, Plaintiffs' allege that Premera affirmatively represented it would provide them with data protection and failed to do so. Plaintiffs identify specific representations that Premera made to its customers and other patients regarding data security. (Compl. ¶¶ 40, 42.) Some of the specific representations alleged in the Complaint include Premera's promise to "maintain[] the confidentiality" of Plaintiffs' Sensitive Information (*id.* ¶ 40), "protect [that

---

[10] *See also Duttweiler v Triumph Motorcycles (America) Ltd*., 2015 WL 4941780, (N.D. Cal. August 19, 2015); *Barber v. Ohana Military Communities, LLC*, 2014 WL 3529766, at *11 (D. Haw. July 15, 2014); *Gray v. BMW of N. Am., LLC*, 22 F. Supp. 3d 373, 385 (D.N.J. 2014); *Falk v General Motors Corp*., 496 F.Supp. 2d 1088, 1098-99 (N.D. Cal. 2007).

information] in a variety of ways," (*id.*), and Premera's "commit[ment] to ensuring the security of our facilities and electronic systems to prevent unauthorized access" to Sensitive Information (*id.* ¶ 42.) At the same time, Premera failed to disclose that it was not maintaining a robust cyber security program to protect Plaintiffs' confidential data.

The Complaint also demonstrates why such representations and omissions were false—Plaintiffs allege that, for example, Premera "failed to implement (or inadequately implemented) information security policies or procedures such as effective employee training on phishing attempts, adequate intrusion detection systems, regular reviews of audit logs and authentication records, and other similar measures to protect the confidentiality of the Sensitive Information it maintained in its data systems," among other related failures to comply with HIPAA, industry standards, and/or its own representations. (*Id.* ¶¶ 63-64.) Because of this contradiction between Premera's representations and its actual data security practices, the representations and omissions "had the capacity to deceive a substantial portion of the public." *Trujillo v. Nw. Trustee Services., Inc.*, 355 P.3d 1100, 1107 (Wash. 2015) (quoting *Panag*, 204 P.3d at 894). Premera's misrepresentations are therefore actionable under the Washington CPA and other states' consumer protection acts.[11]

[11] Premera's heavy reliance on a single paragraph from *Austin-Spearman v. AARP and AARP Services, Inc.*, ---F. Supp. 3d ---, 2015 WL 4555098 (D.D.C. July 28, 2015), is misplaced. (Mot. at 5-6.) In that case, the plaintiff alleged that she paid for the defendant's promise that third parties would not collect personally identifiable information ("PII") through the AARP website. *Id.* at *3. As the court explained, however, the plaintiff's entire theory turned on a section of the defendant's privacy policy that only stated certain third parties would be permitted to collect *non-personally* identifying information—but did not say anything about "the collection or distribution of *PII* at all." *Austin-Spearman*, 2015 WL 4555098, at *6 (emphasis added). Here, the Plaintiffs' allegations do not follow the *Austin-Spearman* formula; rather, they address Premera's repeated and express representations regarding data security and then contrast those representations with its actual data security practices. Thus, while the plaintiff in *Austin-Spearman* tried to construct a promise-by-inference, *Austin-Spearman*, 2015 WL 4555098, at *6, here, Plaintiffs' claims flow directly from Premera's affirmative misstatements and omissions.

c. *Plaintiffs sufficiently allege Premera's actionable omissions regarding its data security practices.*

Next, Premera claims that Plaintiffs do "not provide any particularity" with respect to its alleged omissions. (Mot. at 7.) Instead, Premera suggests Plaintiffs' allegations differ materially from one paragraph to the next—i.e., at one time alleging Premera's failure to disclose its "inadequate security measures," and at another alleging Premera's refusal and/or inability to "protect their Sensitive Information." (*Id.* at 6-7.) But these (and other) allegations are two sides of the same coin. Plaintiffs consistently and specifically allege everything required to put Premera on notice of what it should have—but did not—disclose to its customers: accurate information about the inadequate state of its own data security regime. *See* Section III B 1 (b) *infra*.

It's well-established that a "knowing failure to reveal something of material importance is 'deceptive' within the [Washington] CPA." *Indoor Billboard/Washington, Inc.*, 170 P.3d at 18 (internal quotation omitted). Here, Plaintiffs consistently and specifically identify everything needed to put Premera on notice of its omissions:

- *what* Premera should have told Plaintiffs (that it would not utilize data security in line with its own representations, state and federal law, and industry standards), (Compl. ¶¶ 124, 138)
- *when* and *where* such information should have been conveyed (to Plaintiffs at or before they made the decision to purchase and continue to pay for insurance coverage, or to provide Premera with Sensitive Information), (*id.*)
- *why* Premera was obliged to do so (because it—alone—was in the position "to know the true state of the facts about the design of its security measures because the design of such security measures is not public"), (*id.* ¶¶ 229-237); and
- *why* that information was material to its customers (because the true state of its data security regime would have affected Plaintiffs' decision to purchase or pay for Premera's services, or otherwise provide their Sensitive Information to

Premera), (*id.* ¶¶ 192-205).[12]

Plaintiffs' sufficiently state an actionable omission in support of their first, seventh, and eleventh claims for relief.[13]

d. *Premera's "market rate" causation attack does not address the pleadings.*

Finally, Premera argues that Plaintiffs' causation theory for "fraud-based claims" is based on the market rate for health insurance premiums, which assumes that the retail price of insurance ebbs and flows as it is valued in the market. (Mot. at 8-9.) Like Premera's filed rate doctrine argument, this challenge is based on a misguided premise—Plaintiffs' causation and damages theory does not depend on supposedly fluctuating market rates for health insurance. Rather, it depends on three things: (i) the representations Premera made regarding its promised data security practices, (ii) the information it withheld regarding its actual data security practices, and (iii) Premera's data security practices themselves. (Compl. ¶¶ 8-10.) *But for* Premera's

[12] On these well-pleaded facts, the "problems" identified by Premera's Motion quickly disintegrate. For example, Premera contests Plaintiffs' allegations of materiality because "several plaintiffs do not allege they ever purchased health insurance from Premera." (Mot. at 7.) But Premera's decision to omit material information about its data security practices would have affected those Plaintiffs' decision to provide Premera with their Sensitive Information in the first place (and had they not done so, their Sensitive Information would not have been subsequently compromised). Next, Premera points out that the Policyholder Plaintiffs paid for Premera's services at different times. (Mot. at 7-8.) Premera does not (nor could it) explain why that should matter. Indeed, the only argument Premera offers is one that, yet again, misconstrues the pleadings and misstates that Plaintiffs are, here, insisting that Premera somehow "should have known and told them [as early as 1999] that it would be vulnerable to a cyberattack beginning in May 2014." (Mot. at 8.) Plaintiffs allege only that Premera should have told them of its *actual* data security practices—not that it should have forecasted precise future events. Policyholder Plaintiffs allege had Premera disclosed the relevant information, none of them would have used Premera's services—regardless of *when* they enrolled and/or continued to pay.

[13] Premera points out that the OPM report referenced in the Complaint makes some findings that suggest Premera's data security regime was sufficiently implemented. (Mot. at 8.) But as Plaintiffs—and the media—have noted, the report is also replete with references to Premera's shortcomings. Compl. ¶ 44. This and other evidence will certainly help shape this litigation as the case moves forward, but it hardly demonstrates that, as a matter of law, Plaintiffs cannot state an actionable omission claim here.

representations, omissions, and conduct, *no* Plaintiff would have entrusted Premera with her Sensitive Information, *no* Policyholder Plaintiff would have paid for Premera's woefully inadequate data security, and had Premera implemented its promised data security, *no* Plaintiffs' Sensitive Information would have been exposed.[14] (*Id.* ¶¶ 9-10.)

2. Plaintiffs' breach of contract claim survives because it relies on Premera's express, written promises, which were provided to every member of the Policyholder Subclass.

Premera says that the Policyholder Plaintiffs "have failed to allege facts sufficient to plausibly establish their contracts with Premera contain any promise at all regarding data security." (Mot. at 11.) In support, Premera admits that there *were* contracts between these Plaintiffs and Premera, but suggests that the promises and documents upon which Plaintiffs rely are either not included in those contracts or are too vague to sustain the breach of contract claim. Neither argument warrants dismissal.

The Policyholder Plaintiffs allege the requisite contractual elements of offer, acceptance, and consideration.[15] First, through its policyholder contracts, Premera promised to provide healthcare and data protection services. Premera reduced those promises to writing in several documents (e.g., its Notice of Privacy Practices and Code of Conduct documents) and Plaintiffs paid for such services. (Compl. ¶¶ 161, 163.) Nothing more is required at the pleading stage. *See, e.g., See Resnick*, 693 F.3d at 1329 (reversing dismissal of breach of contract and implied contract claims, which were based on health insurer's notice of patient privacy practices

[14] Further, and contrary to Premera's suggestion, (Mot. at 9), Plaintiffs do not need to plead reliance to support their Washington CPA claim. *Schnall v. AT & T Wireless Services., Inc.*, 259 P.3d 129, 137 (2011) (holding that reliance is not an element of a CPA claim.)

[15] The elements of contract formation don't vary materially between the relevant states. *See, e.g., Bliss v. Southern Pac. Co.*, 321 P.2d 324, 330 (Ore. 1958); Cal. Civ. Code § 1550; *Midgett v. Cook Inlet Pre-Trial Facility*, 53 P.3d 1105, 1114 (Alaska 2002); *Becker v. Washington State University*, 266 P.3d 893, 899 (Wash. Ct. App. 2011).

documents); *Smith v. Triad of Alabama, LLC*, No. 14-cv-324, 2015 WL 5793318, at *14 (M.D. Ala. Sept. 29, 2015) (same). *See also In re Adobe Sys., Inc. Privacy Litig.*, 66 F. Supp. 3d at 1221 (upholding claim for declaratory relief that Adobe breached customer contracts by allegedly violating the data security representations set forth in its online privacy policy).

For its part, Premera faults Plaintiffs for not attaching the supposed "valid, enforceable health insurance contracts issued by Premera" to the Complaint, and then asks the Court to dismiss based on the inference that no contractual obligations relating to data security exist in *those* materials. (Mot. at 11.) This argument is unsupported and premature. In *Smith*, for example, the defendant hospital used an analogous attack and argued that its Notice of Privacy Practices could not form the basis of an express contract. *Smith*, 2015 WL 5793318, at *14. But in upholding the breach of contract claim, the court specifically rejected the defendant's attempt to "determine the nature of the Notice of Privacy Practices" document at the pleading stage. *Id.* *Accord P.E. Sys., LLC v. CPI Corp.*, 289 P.3d 638, 643 (Wash. 2012) ("Mutual assent to definite terms is normally a question of fact for the fact finder.") (Internal citation omitted.) Here, Premera will have the opportunity to contest Plaintiffs' allegations at the summary judgment stage, or trial. It cannot, however, contest Plaintiffs' allegations by referencing un-attached documents and then seeking judicial inferences in its favor, particularly when all such inferences are drawn in Plaintiffs' favor at this stage of the litigation.

Next, Premera attempts to discredit its own written representations as too "indefinite" or "general" to form a contractual promise. However, the test for mutual assent evaluates words of the contract based on "their ordinary, usual and popular meaning unless the agreement as a whole clearly demonstrates a contrary intent." *Lawrence v. Koehler*, 152 Wash. App. 1012, 2009 WL 2939072, at *4 (Wash. Ct. App. Sept. 14, 2009) (internal citation omitted). Further, "[t]here

need only be reasonable certainty of terms for a manifestation of assent," meaning that the terms must "provide a basis for determining the existence of a breach and for giving an appropriate remedy." *Id.* (citing Rest. (2d) of Contracts § 33 (1979)). Here, the terms provided by Plaintiffs are "sufficiently definite," such that the "court [can] decide just what [they mean] and fix exactly the legal liability of the parties."[16] *See Keystone Land & Dev. Co. v. Xerox Corp.*, 94 P.3d 945, 949 (Wash. 2004). For example, in its notice of Privacy Practices (which Plaintiffs allege is part of the Parties' contractual relationship), Premera expressly promises that it is "committed to maintaining the confidentiality of [Plaintiffs'] medical and financial information" before making specific promises to protect Plaintiffs' Sensitive Information in a variety of ways. (Compl. ¶¶ 40, 41 (setting forth additional promises set out in Premera's "Code of Conduct" document)). The promises contained in the notice of Privacy Practices and Code of Conduct are therefore "sufficiently definite" to form the basis of a valid contract. *See Smith v. Trusted Universal Standards in Elec. Transactions, Inc.*, No. 09-cv-4567, 2010 WL 1799456, at *9 (D.N.J. May 4, 2010) (finding on a motion to dismiss that the promises contained in Comcast's privacy policy were sufficiently definite to form the basis of a valid contract).

3. Plaintiffs' breach of implied contract claim relies on the uniform conduct of every member of the Policyholder Subclass providing Sensitive Information to Premera in exchange for its implied promise to protect that data.

Premera says that the Notice of Privacy Practices and the Code of Conduct "form the basis" of the Policyholder Plaintiffs' claim for breach of implied contract and, because Plaintiffs

[16] Premera's articulation of this rule—i.e., that *the documents*, rather than the objective manifestations of the parties, must leave no room for ambiguity and fix the exact legal liabilities of the parties—is too narrow. Unlike *Keystone Land & Dev. Co.*, the contract at issue here—the existence of which Premera itself acknowledges—contains specific promises to protect Plaintiffs' data.

never allege that they read or relied on those documents, their claim fails. (Mot. at 13.)[17] But while these documents strongly *support* Plaintiffs' claim, they are not the sole basis for it. Rather, Plaintiffs allege that, in the alternative to the existence of an express contract, the specific facts and circumstances of the transaction between Premera and the Policyholder Plaintiffs culminated in a meeting of the minds, wherein the parties understood there to be an offer, acceptance, consideration, and mutual assent with respect to data security.

Under Washington law, "[a] contract implied in fact is an agreement depending for its existence on some act or conduct of the party sought to be charged and arising by implication from circumstances which, according to common understanding, show a mutual intention on the part of the parties to contract with each other." *Young v. Young*, 191 P.3d 1258, 1262-63 (Wash. 2008) (internal quotation omitted); *see also*, *DCIPA, LLC v. Lucile Slater Packard Children's Hosp. at Stanford*, 868 F. Supp. 2d 1042, 1053 (D. Or. 2011), (citing *Staley v. Taylor*, 994 P.2d 1220, 1224, n. 6 (Or. App. 2000) ("implied-in-fact contracts arise because an accepted course of conduct would permit a reasonable juror to find that the parties understood that their acts were sufficient to manifest an agreement"); Cal. Civ. Code § 1621("An implied contract is one, the existence and terms of which are manifested by conduct.").

Here, the Policyholder Plaintiffs allege that in order to receive health insurance coverage from Premera, they were required to (i) pay and (ii) hand over their Sensitive Information. (Compl. ¶ 176.) Plaintiffs further allege that they would not have agreed to do either act without an understanding that upon providing Premera with their Sensitive Information, Premera was simultaneously agreeing to safeguard it (and Plaintiffs, in turn, understood they were paying for

---

[17] Premera's second argument against the existence of an implied contract between the parties rests on its assertion that the Notice of Privacy Practices and the Code of Conduct "do not contain any promises regarding data security." (Mot. at 13.) This argument fails for the reasons discussed *supra* in Section III B 3.

that agreement). (*Id.* ¶¶ 9, 129.) And finally, Plaintiffs point to Premera's own privacy documents to support that a meeting of the minds occurred—i.e., Premera understood that, by accepting Plaintiffs' payments and Sensitive Information, it was agreeing (and being paid) to protect it. (*Id.* ¶¶ 4-5.) These facts are more than sufficient to establish the existence of an implied contract, which Premera breached by failing to safeguard Plaintiffs' Sensitive Information. [18]

Premera's reliance on *Krottner* is misplaced. There, the plaintiffs' implied contract claim relied on documents that allegedly memorialized "[t]he terms of the contract,"[19] but—as the Ninth Circuit noted—"[the plaintiffs did] not allege that they read or even saw the documents, or that they understood them as an offer." *Krottner*, 406 F. App'x at 131. Here, in contrast and as explained above, Plaintiffs' implied contract claim stems not only from the documents, but from the entirety of the circumstances precipitating the parties' relationship—including, *inter alia*, (i) the nature of that relationship (insurer and insured), (ii) the mutual understanding that Sensitive Information would not be exchanged absent a promise of protection, and (iii) the fact that Premera's consumer-facing documents *support* that there was a meeting of the minds. (*See* Compl. ¶ 169.)[20] These facts and circumstances readily allege the existence of an implied

[18] *See Smith*, 2015 WL 5793318, at *15 (upholding claim for breach of implied contract in data breach case brought by patient against hospital, and concluding that "Plaintiffs have alleged sufficient facts to allow the claim to proceed to discovery, during which the parties may engage in an investigation regarding the 'circumstances' which show or do not show a mutual intent to contract."); *Enslin v. The Coca-Cola Co.*, No. 14-cv-06476, 2015 WL 5729241, at *14 (E.D. Pa. Sept. 30, 2015) (upholding claim for breach of implied contract in data breach case on allegations that "the [defendants], through privacy policies, codes of conduct, company security practices, and other conduct, implicitly promised to safeguard [plaintiff's] PII in exchange for his employment.").

[19] *Krottner v. Starbucks Corp.*, No. 09-cv-00216, 2009 WL 12701999 at ¶ 102 (W.D. Wash. Apr. 28, 2009) (Amended Class Action Complaint).

[20] Further, in *Krottner*, although the Plaintiffs alleged that the contracts were created by specific documents, the court found that the referenced documents contained no representations about

contract.[21]

4. Plaintiffs' unjust enrichment claim mirrors that approved by the Eleventh Circuit in *Resnick v. AvMed.*

a. *Plaintiffs sufficiently allege the unjust enrichment claim.*

Premera challenges the policyholder Plaintiffs' unjust enrichment claim by arguing that their allegation that a "portion of their premium to Premera was supposed to be allocated to data security" is "arbitrar[y]" and "insufficient even to support Article III standing, let alone entitlement for unjust enrichment." (Mot. at 14.) Again, Premera ignores Plaintiffs' allegations.

The Complaint details (i) the many affirmative representations Premera made about its "commitment" to data security and confidentiality, (Compl. ¶¶ 40-41) (ii) that Plaintiffs would not have purchased health insurance from Premera had Premera revealed its actual data security and confidentiality practices, (*id.* ¶¶ 8-10); (iii) that Premera's data security regime was something Plaintiffs expected and paid for as a part of their health insurance premiums, (*id.* ¶¶ 9, 67, 129); and (iv) because Plaintiffs paid for a service that they did not receive, Premera has been unjustly enriched at their expense, (*id.* ¶¶ 186-191). These allegations more than meet the requirements for unjust enrichment under any state's law.[22]

---

data security. *Id.* In this case, Plaintiffs have referenced multiple documents containing specific representations about data security. *See, e.g.*, Compl. ¶ 40.

[21] Premera also makes the one-sentence argument that Washington's economic loss rule bars Plaintiffs' negligence claim. (Mot. at 14 n.5.) Washington courts no longer apply the economic loss rule; rather, they follow the "independent duty doctrine," which has been limited to "claims arising out of construction on real property and real property sales," making it inapplicable to the instant case. *See Donatelli v. D.R. Strong Consulting Engineers, Inc.*, 312 P.3d 620, 624 (Wash. 2013) (internal quotation omitted).

[22] *See, e.g.*, *Austin v. Ettl*, 286 P.3d 85, 96 (Wash. 2012) (quoting *Young,* 164 Wash.2d at 484–85, 191 P.3d 1258) (under Washington law, "[a] party claiming unjust enrichment must prove three elements: '(1) the defendant receive[d] a benefit, (2) the received benefit is at the plaintiffs expense, and (3) the circumstances ma[d]e it unjust for the defendant to retain the benefit without payment.'"); *Wilson v. Gutierrez,* 323 P.3d 974, 978 (Or. App. 2014) (reciting similar elements under Oregon law); *Darling v. Standard Alaska Prod. Co.*, 818 P.2d 677, 680 (Alaska 1991) (reciting similar elements under Alaska law). Similarly, under California law, "a court may

In fact, this *identical* theory was accepted by the Eleventh Circuit Court of Appeals in *Resnick*. There, and in the wake of a data breach concerning a different health insurer, the plaintiffs sought to recover under an unjust enrichment theory, alleging that "AvMed [a Florida corporation that delivers health care services] [could not] equitably retain [plaintiffs'] monthly insurance premiums—part of which were intended to pay for the administrative costs of data security—because AvMed did not properly secure Plaintiffs' data." *Resnick*, 693 F.3d at 1328. And as with this case, the *Resnick* complaint focused heavily on AvMed's promises to follow HIPAA and otherwise secure the plaintiffs' confidential data. (*See Resnick* Complaint ¶¶ 17-22, a true and accurate copy of which is attached as Exhibit B.) The Eleventh Circuit ultimately held:

> Plaintiffs allege that they conferred a monetary benefit on AvMed in the form of monthly premiums, that AvMed "appreciates or has knowledge of such benefit," that AvMed uses the premiums to "pay for the administrative costs of data management and security," and that AvMed "should not be permitted to retain the money belonging to Plaintiffs . . . because [AvMed] failed to implement the data management and security measures that are mandated by industry standards." Plaintiffs also allege that AvMed either failed to implement or inadequately implemented policies to secure sensitive information, as can be seen from the data breach. Accepting these allegations as true, we find that Plaintiffs alleged sufficient facts to allow this claim to survive a motion to dismiss.

Resnick, 693 F.3d at 1328. *See also Weinberg v. Adv. Data Processing, Inc.*, No. 15-cv-61598, 2015 WL 8098555, at *6 (S.D. Fla. Nov. 17, 2015) (finding *Resnick* "instructive" and upholding claim for unjust enrichment based on payments made to medical billing processor and allegations that expected data security was not provided). The Eleventh Circuit's analysis is directly on point—to say nothing of the other cases to have endorsed this theory of damages.[23]

'construe [a claim for unjust enrichment] as a quasi-contract claim seeking restitution.'" *Astiana v. Hain Celestial Group, Inc.*, 783 F.3d 753, 762 (9th Cir. 2015).

[23] *See*, *e.g.*, *Weinberg*, 2015 WL 8098555, at *6; *In re Adobe*, 2014 WL 4379916, at *15-16; *AOL*, 719 F. Supp. 2d at 111; *In re Target*, 2014 WL 7192478, at *23.

Premera's wholesale discounting of *Resnick* is unwarranted. (Mot. at 15 n.6.) First, the fact that the Eleventh Circuit's analysis was streamlined only reflects the exceedingly straightforward nature of (i) the plaintiffs' allegations, and (ii) the requirements for unjust enrichment. *See Resnick*, 693 F.3d at 1328. Even more telling, however, is Premera's apparent reliance on *Resnick*'s dissenting opinion. There, Circuit Judge Pryor did not question the majority's treatment of the plaintiffs' underlying allegations; rather, he only opined that the claim should have been dismissed because the plaintiff could not "pursue a quasi-contract claim for unjust enrichment if an express contract exists concerning the same subject matter." *Resnick*, 693 F.3d at 1332 (Pryor, C.J., dissenting) (internal quotation omitted). Here, the Policyholder Plaintiffs' unjust enrichment claim is pled in the alternative, thus the *Resnick* dissent inapposite.

b. *Plaintiffs' claim for unjust enrichment does not sound in fraud.*

Next, Premera presses a misguided argument that because Plaintiffs' unjust enrichment claim is "tethered to their allegations of fraud," they must allege "reliance on the statements they allege are fraudulent." (Mot. at 15.) However, Plaintiffs' unjust enrichment claim has *nothing* to do with a claim for fraud and, as such, allegations of reliance are not required.

Premera's reliance on *Cleary v. Philip Morris, Inc.*, 656 F.3d 511 (7th Cir. 2011) to establish that such allegations are required is misplaced. In that case, a group of cigarette smokers sought to recover a benefit conferred on Philip Morris (sales revenue) on an unjust enrichment theory, relying only on a supposed "legal right as consumers to be informed of the true nature and risks of the defendants' products." *Id.* at 519. But, as the Seventh Circuit noted, the plaintiffs there did not allege that the breach even harmed the putative class, which included persons who would have bought cigarettes knowing of their "addictive and harmful nature." *Id.* Here, in contrast, Plaintiffs do not claim violation of a vague and abstract "right to be informed;"

rather, they focus on actual services (data protection) that Premera promised to, but did not, provide. (Compl. ¶¶ 8-10.) Moreover, unlike the speculative or disparate impact on plaintiffs in *Cleary*, Premera's failure to provide the promised data protection services affected all the policyholder Plaintiffs in the same way. Thus, because *all* the policyholder Plaintiffs paid for services they did not receive, they *all* were harmed in the same way—and, having accepted money for services that it did not provide, it would be unjust for Premera to keep the Policyholder Plaintiffs' money. (*Id.* ¶¶ 186-191.) Such allegations provide the "connection between the defendants' [conduct] and a detriment to the plaintiffs" that the Seventh Circuit found lacking in *Cleary*. 656 F.3d at 519.

Accordingly, because (i) Premera has retained money obtained in payment for services that it promised but never provided and (ii) the Policyholder Plaintiffs never would have purchased Premera's insurance in the first place, had Premera been forthright about its *actual* data security practices, Plaintiffs' unjust enrichment claim should stand.

5. Plaintiffs' breach of fiduciary duty claim stems from the one-sided nature of the parties' relationship, wherein Premera placed itself in a position of trust.

Premera also moves to dismiss Plaintiffs claims for breach of fiduciary duty under the general premise that "courts have routinely rejected" imposing a fiduciary duty based on failure to protect information. Focusing on Washington law, Premera argues that "no Washington court has recognized a claim for breach of fiduciary duty by an insured." *Id.* Premera ignores the fact, however, that Washington imposes a quasi-fiduciary duty on insurers *with respect to coverage decisions*. Premera's duty with respect to coverage decisions is not determinative of its fiduciary duty with respect to confidential information.

Washington recognizes two categories of fiduciary duty. A fiduciary duty *as a matter of law* exists where "the nature of the relationship between the parties is historically considered

fiduciary in character[.]" *Alexander v. Sanford*, 325 P.3d 341, 363 (Wash. Ct. App. 2014) (quoting *McCutcheon v. Brownfield*, 467 P.2d 868 (Wash. 1970)). On the other hand, even where a fiduciary duty as a matter of law does not exist, "a fiduciary relationship *arises in fact* when there is something in the particular circumstances which approximates a business agency, a professional relationship, or a family tie, something which itself impels or induces the trusting party to relax the care and vigilance which he otherwise should, and ordinarily would, exercise." *Id.* (quoting *Hood v. Cline*, 212 P.2d 110 (Wash. 1949)). This type of fiduciary relationship may exist where one party has superior knowledge and thereby induces reliance on that knowledge by the other party. *Pope v. Univ. of Wash.*, 852 P.2d 1055, 1063 (Wash. 1993).

Here, Plaintiffs have alleged the existence of a fiduciary relationship between the Parties as a matter of fact. Premera requires Plaintiffs to disclose personal information, represents that it has the knowledge and ability to protect that information, and has superior knowledge regarding the nature and sufficiency of those protections than do Plaintiffs. Plaintiffs entrusted their most personal and private medical information to Premera so that Premera has the information to pay Plaintiffs' medical providers and ensure Plaintiffs' continued good health. Plaintiffs are justified in trusting that when they disclose their private information to Premera, Premera will use it only for the agreed purposes and will protect the confidentiality of that information as a fiduciary.[24]

---

[24] These allegations distinguish this case from *Lovell v. P.F. Chang's China Bistro, Inc.*, --- Fed. App'x ---, 2015 WL 4940371 (W.D. Wash. Mar. 27, 2015). The *Lovell* court dismissed the data breach plaintiff's breach of fiduciary duty claim, citing the fleeting nature of the relationship between the parties (restaurant and customers), the defendant's lack of representations to plaintiff regarding security protocols, that defendant did not require the use of credit cards or do anything to induce plaintiff to use a credit card, and plaintiff used his credit card for his own convenience. *Id.* at *4. Unlike *Lovell*, here Premera has an ongoing relationship with Plaintiffs and makes representations about its security protocols. Further, Plaintiffs did not voluntarily give their personal information to Premera without inducement—divulging of personal information is a necessary component of health insurance. For the same reason, Plaintiffs did not divulge their personal information for their own convenience, but because Premera required it. The information Plaintiffs provided to Premera was far more sensitive and deserving of protection

Finally, Premera says the Court should draw a distinction between Plaintiffs for whom Premera was their insurer, Plaintiffs for whom Premera served as third party administrator, and Plaintiffs who were insured by other Blue Cross plans but received treatment in Washington. (Mot. at 17.) This is a distinction without a difference. The existence of a fiduciary relationship in fact does not depend on the type of relationship between the parties (attorney-client, insurer-insured, etc.). Rather, it depends on the circumstances of the relationship. And here, the allegations giving rise to the duty apply equally to Premera with respect to its relationship with each "group" of Plaintiffs, as they all supplied Sensitive Information to Premera regardless of whether they were insureds.

6. Plaintiff Hansen-Bosse states a claim under the CMIA.

Premera argues that Plaintiff Hansen-Bosse's CMIA claim should be dismissed because Plaintiffs failed to allege that their medical information was "viewed" by the hackers. But Plaintiffs allege, and Premera admits, that medical information within the meaning of the CMIA[25] was disclosed in the data breach, "including clinical information."[26] Plaintiffs also

---

than credit card numbers. Finally, unlike the decision to eat out at a restaurant, as a matter of federal law, individuals have no choice but to purchase health insurance. *See* 26 U.S.C. § 5000A.

[25] Under the CMIA:

> "Medical information" means any individually identifiable information, in electronic or physical form, in possession of or derived from a provider of health care, health care service plan, pharmaceutical company, or contractor regarding a patient's medical history, mental or physical condition, or treatment. "Individually identifiable" means that the medical information includes or contains any element of personal identifying information sufficient to allow identification of the individual, such as the patient's name, address, electronic mail address, telephone number, or social security number, or other information that, alone or in combination with other publicly available information, reveals the individual's identity.

Cal. Civ. Code § 56.05(j).

[26] *See* https://www.premera.com/wa/visitor/about-the-cyberattack/?WT.z_redirect= www.premera.com/cyberattack/ (last visited Dec. 2, 2015). (*See also* Compl. ¶ 1 (alleging Defendant disclosed medical information and "protected health information as defined by . . . HIPAA" in the data breach).)

allege that the information which the hackers acquired in the data breach—including medical information—has not only been "viewed" by the hackers, but that it already has been misused in a variety of ways to harm class members including, to date, a number of fraudulently filed tax returns and fraudulent attempts to open lines of credit in victims' names. (Compl. ¶¶ 78-100.)

These allegations negate Premera's reliance on *Sutter Health v. Superior Court*, 174 Cal. Rptr. 3d 653 (Cal. Ct. App. 2014), and *Regents of Univ. of California v. Superior Court*, 163 Cal. Rptr. 3d 205 (Cal. Ct. App. 2013). Those courts dismissed CMIA claims because those plaintiffs did not allege that their stolen information actually was "viewed" by the thief. *Sutter*, 227 Cal. App. 4th at 1550; *Regents*, 220 Cal. App. 4th at 554.[27] But here, Plaintiffs allege that their medical information was disclosed in the data breach, that the hackers who perpetrated the breach have been misusing Plaintiffs' information in a variety of ways, that they will remain vulnerable to misuse of their Sensitive Information "for years" to come, and that medical information is particularly valuable to, and sought after by, criminals. (Compl. ¶ 72, 75).[28]

In cases more analogous to the present scenario, courts have denied motions to dismiss CMIA claims. For instance, where hackers perpetrated a data breach and acquired Sony employees' medical information, the court refused to dismiss plaintiffs' CMIA claim. *Corona*,

[27] Unlike the present action, where Plaintiffs allege that "their Sensitive Information was specifically targeted by hackers seeking to steal consumer data" (Compl. ¶ 8), Premera's cited cases did not consider such purposeful data breaches by hackers. In *Regents*, 220 Cal. App. 4th at 554, "an encrypted external hard drive containing some [patients'] personally identifiable medical information had been stolen as part of a home invasion robbery," and in *Sutter*, 227 Cal. App. 4th at 1552, "someone broke into an office of Sutter Health and stole a desktop computer" containing "medical records of more than four million patients . . . in password-protected but unencrypted format."

[28] Premera also relies on *Eisenhower Med. Ctr. v. Superior Court*, 172 Cal. Rptr. 3d 165 (Cal. Ct. App. 2014), but that case did not concern disclosure of medical information akin to that disclosed by Premera in its data breach. In *Eisenhower Med. Ctr.*, a "computer was stolen . . . containing an index of over 500,000 persons to whom [defendant] had assigned a clerical record number." *Id.* at 166. The "index did not contain medical information within the meaning of the CMIA.'" *Id.* at 167.

2015 WL 3916744, at *8. And in *Falkenberg v. Alere Home Monitoring, Inc.*, No. 13-cv-00341, 2015 WL 800378, at *3-4 (N.D. Cal. Feb. 23, 2015), the court denied a motion to dismiss a CMIA claim where plaintiffs alleged their medical information was disclosed through a laptop theft, resulting in a variety of injuries like Plaintiffs' alleged injuries in this case, including attempted financial identity theft. The Motion to dismiss Plaintiff Hansen-Bosse's CMIA claims should be denied.

7. Plaintiffs adequately allege damages flowing from Premera's delayed notification of the data breach.

Premera concedes that three Plaintiffs have alleged "damages flowing from an actual misuse" of their Sensitive Information during the time when Premera failed to notify class members about the data breach, and thus its Motion should be denied as to Plaintiff Black's, Lynch's, and Prakash's claims under Washington's data breach notification statute, RCW § 19.255.010. (Mot. at 20.) Premera's assertion that the "remaining twenty-five plaintiffs have not alleged any injury causally connected" to Premera's delayed notification of the breach ignores the income tax fraud allegations of Plaintiffs Smith, Bushman, Allred, Foulon, and Webster, all of which occurred prior to Premera's March 2015 breach notification. (Compl. ¶¶ 89, 91, 94, 99.) These Plaintiffs also have alleged sufficient damages from the misuse of their Sensitive Information, and Premera's Motion to dismiss their RCW § 19.255.010 claims should fail.[29]

Similarly unavailing is Premera's argument that immediate notification was not required because Premera owns the subject data that was breached, and RCW § 19.255.010(2) only

[29] Premera's reliance on *In re Barnes & Noble Pin Pad Litig.*, 2013 WL 4759588 (N.D. Ill. Sept. 3, 2013) and *Green v. eBay, Inc.*, 2015 WL 2066531 (E.D. La. May 4, 2015) ignores the fact that Plaintiffs have suffered actual damage as a result of Premera's notification delay, damages that could have been avoided or mitigated had Premera notified Plaintiffs sooner. *See Barnes & Noble*, 2013 WL 4759588, at *3 (violation insufficient to establish standing where the plaintiffs alleged no actual misuse or damages caused by the breach, let alone damages specifically associated with delayed notification); *see also Green*, 2015 WL 2066531 at *3 (same).

applies to licensees. (Mot. at 20 n.9.) Whether Defendant is an owner or licensor of Plaintiffs' Sensitive Information is a question of fact which should not be determined at the motion to dismiss stage. However, Plaintiffs certainly disagree that Premera "owns" the most sensitive details of their personal medical care, rather than being entrusted as a fiduciary with the "use" of that information to benefit Plaintiffs in seeking medical treatment.[30]

Finally, even if Plaintiffs are precluded from pursuing monetary damages under RCW § 19.255.010 and other state data breach laws. Plaintiffs nonetheless are entitled to pursue injunctive relief under these statutes. *See In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 996 F. Supp. 2d 942, 1010 (S.D. Cal. 2014) (denying motion to dismiss, reasoning that "Plaintiffs may pursue their injunctive relief claims under [Cal. Civ. Code] Section 1798.84(e), which affords relief when a 'business violates, proposes to violate, or has violated' the [CRA].'"). Premera's Motion should be denied.

IV. CONCLUSION

Whether from the misuse they have endured, the loss of their private information, or from their overpayment for data protection services that Premera promised but never delivered, Plaintiffs allege sufficient facts demonstrating that they suffered cognizable losses from Premera's failure to safeguard their Sensitive Information. For these and the reasons above, Premera's Motion should be denied.

---

[30] Premera's Motion is silent as to its violations of other states' data breach notification laws. Without limitation, the allegations of Plaintiffs Hansen-Bosse, Forseter, Kaplowitz, and Ailey assert claims under Cal. Civ. Code § 1798.80, *et seq.*, Md. Code Ann., Commercial Law §14-3504, *et seq.*, N.J. Stat. Ann. § 56:8-163, *et seq.*, and Tex. Bus. & Com. Code Ann. § 521.053, *et seq.* (Compl. ¶81, 83, 86, 90, 108, 207-12), respectively. Premera has not challenged Plaintiffs' claims under the other states' data breach notification laws (*See* Compl. ¶ 210) and, therefore, Plaintiffs' claims under these states' data breach notification statutes should not be dismissed.

DATED December 30, 2015.

TOUSLEY BRAIN STEPHENS PLLC

By: *s/Kim D. Stephens*
Kim D. Stephens, OSB No. 030635
Christopher I. Brain, admitted *pro hac vice*
Chase C. Alvord, OSB No. 070590
Jason T. Dennett, admitted *pro hac vice*
1700 Seventh Avenue, Suite 2200
Seattle, WA 98101
Tel: (206) 682-5600
Fax: (206) 682-2992
Email: cbrain@tousley.com
kstephens@tousley.com
calvord@tousley.com
jdennett@tousley.com

Interim Lead Plaintiffs' Counsel

STOLL BERNE LOKTING & SHLACHTER P.C.

By: *s/ Keith S. Dubanevich*
Keith S. Dubanevich, OSB No. 975200
Steve D. Larson, OSB No. 863540
Mark A. Friel, OSB No. 002592
209 SW Oak Street, Suite 500
Portland, OR 97204
Tel: (503) 227-1600
Fax: (503) 227-6840
Email: kdubanevich@stollberne.com
slarson@stollberne.com
mfriel@stollberne.com

Interim Liaison Plaintiffs' Counsel

Ari J. Scharg
ascharg@edelson.com
EDELSON PC
350 North LaSalle Street, Suite 1300
Chicago, Illinois 60654
Tel: 312.589.6370
Fax: 312.589.6378

Tina Wolfson
twolfson@ahdootwolfson.com
AHDOOT AND WOLFSON, PC
1016 Palm Avenue
West Hollywood, CA 90069
Tel: 310.474.9111
Fax: 310.474.8585

James Pizzirusso
jpizzirusso@hausfeldllp.com
HAUSFELD LLP
1700 K. Street NW, Suite 650
Washington, DC 20006
Tel: 202.540.7200
Fax: 202.540.7201

Plaintiffs' Executive Leadership Committee

CERTIFICATE OF SERVICE

I hereby certify that on this day I electronically filed the foregoing document with the Clerk of the Court using the CM/ECF system which will send notification of such filing to all counsel of record.

s/ Kim D. Stephens
Kim D. Stephens